Digital Tokens: A Scheme for Enabling Trust Between Customers and Electronic Marketplaces

Balaji Rajendran, Mohammed Misbahuddin, S. Kaviraj and B. S. Bindhumadhava

Abstract In electronic marketplaces, when the supply of a particular product is limited, and when there is a huge demand for the same, the questions of transparency and integrity prop up. We propose Digital Tokens—defined using proven cryptographic techniques—as a mechanism to assure trust for customers, and issued by a reliable, transparent and third-party intermediary, called digital token service provider (DTSP). The digital tokens are issued to a customer on behalf of a vendor and could be authenticated by both Vendor and the DTSP. This paper details the architecture involving the DTSP, protocols for communication, implementation details, the potential uses and benefits of the system and performance evaluation of such a system.

Keywords Digital token · Timestamp · DTSP · Digital token service provider Certifying authorities · Electronic market place

1 Introduction

The electronic marketplaces [1] have been witnessing huge demand for select brands of products such as mobile phones from customers. These electronic marketplaces have limited stock of the products, primarily owing to the constraints of

B. Rajendran (✉) · M. Misbahuddin · S. Kaviraj · B. S. Bindhumadhava
Computer Networks and Internet Engineering (CNIE) Division,
Centre for Development of Advanced Computing (C-DAC),
Electronics City, Bangalore 560100, India
e-mail: balaji@cdac.in

M. Misbahuddin
e-mail: misbah@cdac.in

S. Kaviraj
e-mail: skaviraj@cdac.in

B. S. Bindhumadhava
e-mail: bindhu@cdac.in

S. Bhalla et al. (eds.), *Intelligent Computing and Information and Communication*,
Advances in Intelligent Systems and Computing 673,
https://doi.org/10.1007/978-981-10-7245-1_48

the supplier, and therefore release the product in batches, which leads to huge competition among potential buyers as they easily outnumber the available quantity, and many buyers return disappointed, as the entire stock goes off in a flash.

We propose a mechanism of Digital Token, wherein a Digital Token is issued to the customer by a trusted intermediary, on behalf of the vendor. The token is then presented by the customer to the vendor, which can be verified for its authenticity and validity by both the intermediary and the vendor. The trusted token can also be validated by the customer if required, by communicating with the intermediary. This mechanism establishes the much-needed trust between the customer and the vendor.

Digital Tokens are useful, whenever the demand is more and supply is less, and when the buyers need a reliable and trustable intermediary. In general, the concept could be applied to any real-life token system, and the potential applications are many as detailed in the later sections of this paper. The benefits of the digital token-based system include: the introduction of a trustable third party that could be relied by the buyer and because of which the vendor relies on it—as it brings in transparency and the vendor can offload the complexities involved in generating the tokens, authenticating and validating them and also will have lesser loads on its servers.

This paper explains the elements of such a Digital Token, the process of authentication and validation of a Digital Token that can be carried out by Vendor and the Intermediary, the protocols for communication between the three parties—Customer, Vendor (eMarketplace) and the Intermediary (referred as the DTSP—Digital Token Service Provider), and finally, the implementation detailing the experimental setup and study of performance issues.

2 Related Work

The concept of Digital Token as a cryptographically encoded message with Digital Time Stamps has not been mentioned elsewhere, although the reference of tokens has been widely used in the literature.

However, the concepts of Digital timestamping [2] as a time validation methodology has been described and used in several PKI-based applications, including e-Tendering, e-Auction, etc. Digital timestamping is comprehensively described in the IETF RFC 3161 standard [3]. The format of timestamping request and the response are detailed. Digital timestamping as a service has been offered by several vendors all over the world, with most of the vendors offering the core CA (Certifying Authority) services.

Digital Watermarking is a technique used for copy-protection of media content, by tracking any unauthorized distribution of the digitally watermarked content. A buyer–seller watermarking protocol [4] was proposed, in such a way that neither

the buyer will be able to distribute the watermarked contents received from the seller, nor the seller would be able to create unauthorized copies of the buyer watermarked contents. The proposed technique uses digital signatures and encryption for its protocol. Holmquist et al. [5] proposed the concept of tokens as a physical object required to access digital information. A Credit card company aimed to replace the Credit Cards with a Digital Token [6]. The concept of Token based Secure Electronic Transaction [7] was proposed by Rajdeep et al., which focused on the customers can be sure about the trustworthiness of the Seller before indulging any transaction, they also mentioned that faulty transactions never take place by implementing token-based SET mechanism in electronic commerce sites.

Matsuura et al. [8] proposed digital timestamp mechanism for dispute settlements in electronic commerce by providing long-lived authenticity and archiving by the server. Shazia et al. [9] explained the importance of E-commerce security, implementing PKI, digital signature and certificate-based cryptographic techniques in E-commerce security.

3 Proposed System: Architecture and Processes

3.1 Entities

There are three entities involved in this System: Customer—who is interested in buying a product; Vendor—selling a product through an electronic marketplace; DTSP—Digital Token Service Provider—a trusted intermediary for both the Customer and the Vendor, who issues Digital Tokens, and who can verify the authenticity and time validity of a token.

3.2 Digital Token

A Digital Token is a cryptographic entity derived from customer's identity, time value and a timestamp by the DTSP. The time value indicates the time validity of the token, the timestamp mentions the time the token was generated that will uniquely identify a transaction.

3.3 Architecture

Figure 1 illustrates the architecture containing the overall sequence of communications between Customer, Vendor and DTSP detailing the life cycle of a Digital Token.

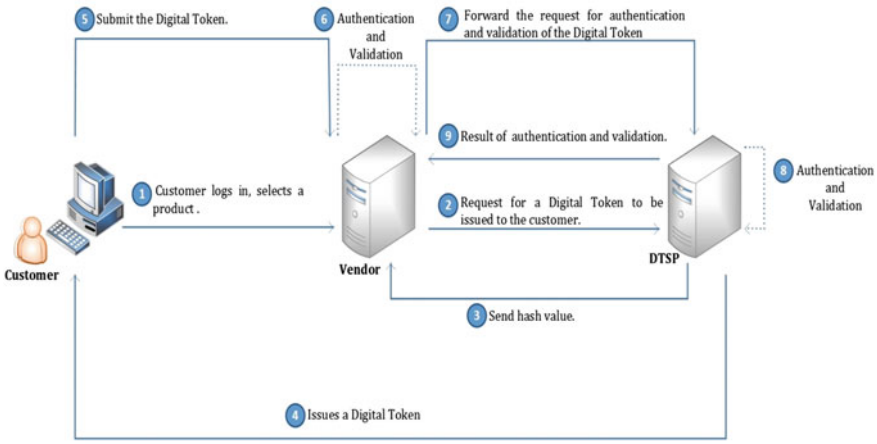

Fig. 1 Digital token life cycle

3.4 Processes

The system is comprised of two main processes: One, issuance of a token to a customer, on behest of the Vendor; Two, authentication and validation of the digital token—which can be either carried out by the Vendor or by the DTSP on request.

Process 1: Digital Token Issuance
Step 1: This is a base operation, wherein the customer visits the vendor website (typically an online marketplace) and selects a particular product, and requests for an advanced registration or booking. The vendor then records the request and assigns a time slot—during which the customer has to appear for buying of the product—and sends a request to DTSP to issue a Digital Token to the customer on its behalf. During the above process, the vendor constructs the Digital Token request—DTRQ, which consists of customer's id (UID), start time (ST) and end time (ET). DTRQ is then digitally signed by the vendor and sent to the DTSP.
Step 2: DTSP, upon receipt of the request—DTRQ, verifies the authenticity and integrity of the request by verifying the digital signature sent along with the request. If authenticated successfully, a timestamp value is obtained and sent as a response to the request in a cryptographically hashed form [10], as follows:

H = Hash (Customers ID + Start Time + End Time + TimeStamp + Nonce);
Here, the nonce represents a random secret value generated by DTSP. Now the DTSP proceeds to generate a digital token, by digitally signing the request and response as

DT = <S, H> where S = Digital Sign (H)
Therefore, a Digital Token is a digital signature of the DTSP along with the generated Hash, which is sent to the customer. Figure 2 illustrates the Token issuance process:

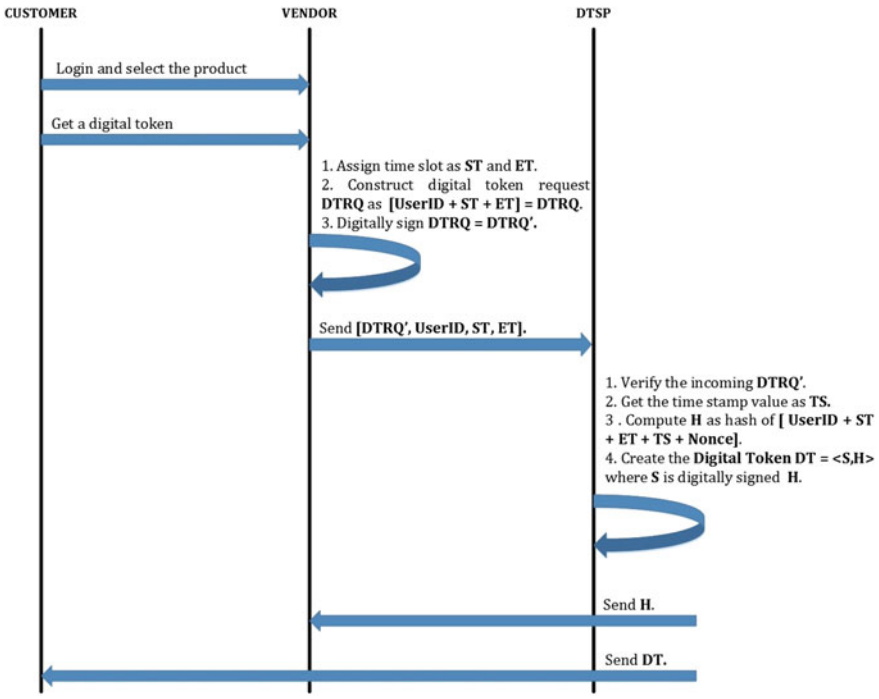

Fig. 2 Digital token issuance process

Process 2: Authentication and Validation of Digital Tokens

The authenticity check will tell whether the token has been really issued by the DTSP to the particular customer in question, on behalf of the said vendor. The validation will have two cases—one, the customer presenting it at the right time slot, two—the customer presenting either before time or after time—the latter case being an expired token, but both invalid.

Step 1: The customer logs into the vendor site (at the specified time slot) and uploads the Digital Token, received from the DTSP corresponding to a particular product. The authenticity and validity of the token can now be carried out either by the vendor or by the DTSP.

Step 2(a): *Authentication and Validation by the Vendor:* The vendor verifies the Digital Signed Hash from Digital Token by using the public key of the DTSP. The vendor then searches his database for the H value from DT using the customer's ID as a filter, and if a match is found then the token is authentic—i.e. the token has been issued by the DTSP, for the particular customers. The vendor will also be able to retrieve the time values—start time and end time and validate the token for the time, and if found to be valid, the vendor may permit the customer to proceed for the subsequent steps involved in buying a said product. Figure 3 illustrates the process of authentication and validation carried out by the vendor.

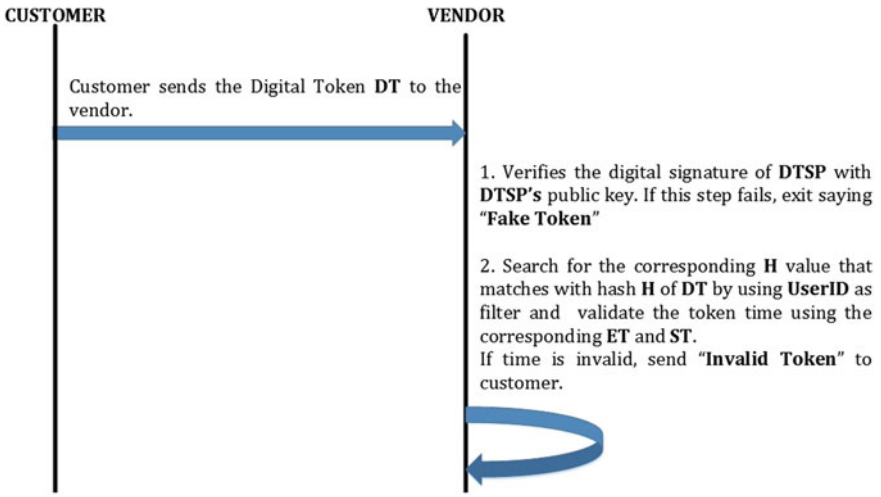

Fig. 3 Authentication and validation of digital token by vender

Step 2(b): *Authentication and Validation by the DTSP*: The vendor can decide to offload the authentication process to the DTSP, by simply forwarding the digital token. In such a case, the DTSP will receive the digital token presented by the customers, and the customer's id from the vendor. The DTSP will then verify the digital signature from Digital Token using its public key. Now the DTSP will search its database of active tokens issued at behest of the particular vendor, containing H value from DT using the Customers Id as the filter. If found, the token is authenticated successfully, meaning the token has been issued by the DTSP only, and then the time validation can be done by fetching the corresponding start and end time. The result of the validation will then be communicated to the vendor by the DTSP. Figure 4 illustrates the process of authentication and validation carried out by the DTSP.

4 Implementation

A prototype implementation has been developed using Java EE wherein the entities —Vendor and DTSP are modelled as distinct entities as in real situations, and cryptographic operations are carried out with the native Java Crypto libraries.

4.1 Features and Assumptions

1. The DTSP does not store any product information that the customer is buying, therefore helping to protect the privacy.

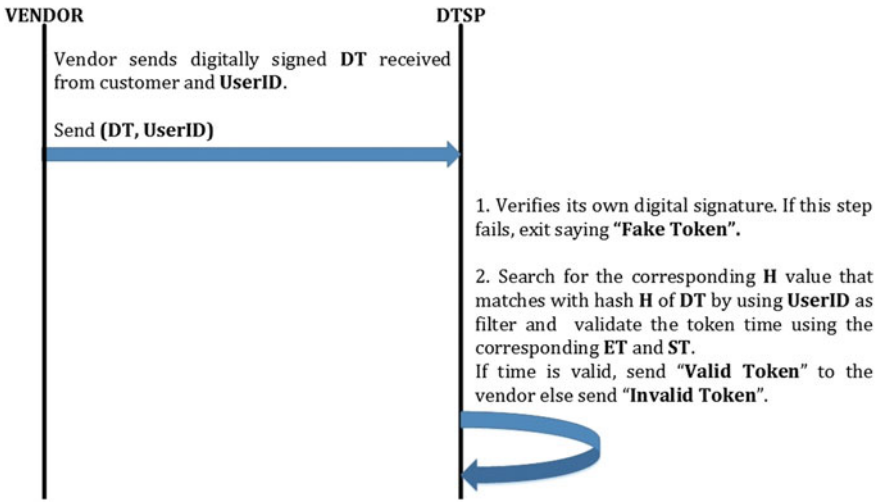

Fig. 4 Authentication and validation of digital token by DTSP

2. The DTSP is running a timestamp server or at least has an access to a timestamp service that will give a reliable time.
3. There is binding between the customer and a Digital token, as DTSP uses customer identification (CustomersID) information supplied by the vendor. The Customers Id is assumed to be an email address as typically is the case with most vendors.
4. The start time could be null by default, which means that the customer can buy the product after it is open for sale at any time, but before the end time.
5. A customer can obtain a digital token only for one quantity of a product at a time. If more quantities are required, the customer has to obtain those many digital tokens.

4.2 Digital Token Encoding

The digital token created by the DTSP on behalf of the vendor is emailed as a file to the customer. The digital token as described above is actually a signature of the DTSP on a message containing a time stamp. The digital signature is encoded in the standard Base64 [11] format, and emailed to the customer. Upon receipt of the token, for authentication and validation, either by the vendor or by the DTSP, both have to decode it back to the standard bytes for further processing. A sample digital token is given below:

–Begin Signature–
ckvZu-
oSlH3+670PLu2QwoXUd2COoKt9GkutCBVi9nmyyeSII/pNDCPLlg8/2U
+WrjfG62
HJatUs-
vaAY2G4UUfvFsipVQFDmH4K4PftSaHdG+/RD+VIG43n5lZxerUy0oB/
QfCKTLAk9aHw/KrF8NxQTdnckw8gkTtzfo/t1LjOw=
–End Signature–
–Begin Hash–
bf65c0043aec52ec26f4c67014e5960d40a4755d
–End Hash—

4.3 Schema

The schema of the **DTSP** is given as below:

{ID, VendorID, CustomersID, StartTime, EndTime, Timestamp, Hash, Status}

As it can be observed, the following information comes from the vendor—CustomersID, StartTime, EndTime and VendorID—each vendor is assigned a unique ID by the DTSP. The Hash value computed by the DTSP would be used for searching for a token, in case if the same customers had booked for multiple quantities of the same product or booked for different products from the same vendor having overlapping timeslots.

We use MongoDB [12] for storing the data, as it yields readily itself to JSON format so that it could be used for communications straightaway. The status field is used to store the status of the record/digital token—Active, Expired, etc. All expired tokens are moved out periodically to separate databases, keeping only the active ones, and grouped by vendor to improve the search performance of DTSP. A sample of a fully constructed a document with the DTSP would look as follows:

```
DTSP Document:
{
``_id'' : ObjectId(``55e7f79d8ad5d90404000029''),
``VendorId'':64,
``CustomersId'':``xyz@abc.in'',
``StartTime'':new Date(``3-9-2015 12:30:00''),
``EndTime'':new Date(``3-9-2015 19:30:00''),
``TimeStamp'':new Date(``25-8-2015 16:35:00''),
``Hash'': ``bf65c0043aec52ec26f4c67014e5960d40a4755d'',
``Status'':``Active''
}
```

The schema at the **Vendor** for the purposes of Digital Tokens is given as below:

{ID, CustomersID, ProductID, StartTime, EndTime, Hash, Status}

As it can be observed, the vendor has details of the customers, along with the product information that the customers are seeking to book, and also the time in which the vendor wants to allow the customers to actually buy the product. The vendor can set the 'StartTime' as NULL, if he wants to only set the end time to the customer. The Hash value is obtained from the DTSP, which is a combination of the above information plus the timestamp.

```
Vendor Document:
{
``_id'':ObjectId(``55e7f79d8ad5d90404000029''),
``CustomersId'':``xyz@abc.in'',
``ProductId'':M101256,
``startTime'':new Date(``3-9-2015 12:30:00''),
``EndTime'':new Date(``3-9-2015 19:30:00''),
``Hash'': ``bf65c0043aec52ec26f4c67014e5960d40a4755d'',
``Status'':``Active''
}
```

4.4 Communication Between Vendor and DTSP

The Vendor communicates with DTSP during the process of token issuance and during the process of authentication and validation. During Issuance, the vendor opens up a connection with the DTSP, and communicates its identity, the customer identity information and the time slot, as a key-value pair in JSON format and redirects the customer to the DTSP's page. The Vendor then waits to listen from the DTSP for the corresponding H value and closes or resets its connection with the customer.

In the process of authentication and validation, if the vendor decides to offload the process to the DTSP, the vendor has to communicate its and the customer's identity information, and wait for the result. If a successful result is announced by the DTSP, then the vendor puts the customer through the subsequent process of buying the product. It may be noted that the DTSP communicates the results only with the vendor, which will be useful for the latter to detect any multiple attempts by an attacker to hog the resources by sending fake tokens, or expired tokens.

4.5 Screenshots

A sample of the screenshots depicts the flow of the process as illustrated in Fig. 5.

Fig. 5 Sample screenshots

5 Performance Analysis

The performance is analyzed by looking at the time it takes to create a digital token, and the time it takes to authenticate and validate a token.

5.1 Time Taken to Generate a Digital Token

Generating a Digital Token is carried out by the DTSP and involves the following steps, and the average time for each activity is given in Table 1. As it can be seen, approximately 470 digital tokens can be created in less than a minute, by a system that is not fully optimized for this activity. The mailing of digital tokens to the customer is considered as a separate process, outside of the critical sections affecting the performance of the system. Also, it may be noted that the timestamps are obtained from a dedicated timestamping service that implements the RFC 3161, and hence, the time taken to obtain it is higher than obtaining the local server time value.

5.2 Time Taken for Authentication and Validation

The authentication and validation can be carried out by either the Vendor or the DTSP and the logic is same—verification of the presented Digital token with the

Table 1 Average time taken for generation of a digital token

S. No.	Activity	Average duration (in ms)
1	Generating the timestamp—typically done through a timestamping server operated by the DTSP	122
2	Creating the hash of all the values {CustomersID, StartTime, EndTime, TimeStamp, Nonce}	0.75
3	Creating the signature by encrypting the Hash created in step 2 with its private key	4.01
4	Encoding the signature in base64 format and writing into a file	1.66
Total		128.42

Table 2 Average time taken for authentication and validation of a digital token

S. No.	Activity	Avg. time (in ms)	Remarks
1	Reading and decoding the signature given in base64 format	0.55	Failure at this step can mean the token is corrupted
2	Verification of the signature using public key of DTSP	2.56	Failure here means, the customers may be presenting a fake token
3	Searching for the H value (part of DT)	0.26	Failure here means, the customer has presented an invalid token
4	Perform time validation	0.01	Failure here means, the token has been presented before time (as expired tokens have been moved to different database and in that case would be eliminated in previous step)
Total		3.38	

public key of DTSP and search for the record matching the Hash value, and if found then perform the time validation. The above steps and time taken are given below in Table 2.

In the case of authentication and validation, failure is possible at each and every step, and failure at an earlier stage is better than at the later stage—as the latter stages will add to the cost of time. Step 3 and 4 have been optimized using efficient data structures and clean-up techniques.

5.3 Analysis

Following observations can be made from the above experiments:

1. The process of digital token issuance is costlier than the process of authentication and validation.

2. In the event of authentication and validation by DTSP, the overheads involved in communication between the vendor and the DTSP is primarily determined by the latency factor, rather than the process itself.
3. The cryptographic operations–especially the encryption and decryption are relatively faster.

When the vendor is experiencing peak-traffic loads, it may offload the process of authentication and validation of digital tokens to the DTSP, but in such scenarios the vendor may have to take into account the latency delays also, as the time required to do the authentication and validation is meagre 3.38 ms, which means an approximate 17,000 digital tokens could be evaluated in less than a minute. The vendor can use the above value as guidance to timeslot the customers accordingly.

6 Conclusion and Future Work

In this paper, we presented the concept and process of a Digital Token, issued by a trusted intermediary, playing the role of a DTSP—a role that could be played by a Certifying Authorities (CA) which could probably add to another business or revenue line to their existing services—the Digital tokens being issued to the customer who is attempting to buy a high-demand product or service from an electronic marketplace. The DTSP can conduct audit trails of the digital tokens issued, authentication and validation done by it and can publish the same.

The process could have been strengthened for the better by having a tight binding between a digital token and the customer, but then the customer should have a mechanism to apply their digital signature. Server-based digital signing approaches like eSign [13] could be used for high-value transactions. This approach can be extended to create a competitive market place by decoupling the tokens from the market places. Therefore, in our future work, we aim to shift the balance in binding proportions wherein we envisage a strong binding between the customer and the token, while a light binding between the token and the vendor or eMarketplace.

References

1. Sonja Grabner-Kraeuter, The Role of Consumers' Trust in Online-Shopping, July 2002, Journal of Business Ethics. http://link.springer.com/article/10.1023/A:1016323815802
2. S. Haber, WS. Stornetta, "How to Time-Stamp a Digital Document" Springer Berlin Heidelberg, pp. 437–455, 1991
3. C Adams, P Cain, D Pinkas, R Zuccherato, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), 2001 – IETF RFC 3161 - https://www.ietf.org/rfc/rfc3161.txt
4. "A Buyer-Seller Watermarking Protocol", Nasir Memon, Ping Wah Wong, IEEE Transactions on Image Processing, pp: 643–649, 2001

5. L. Holmquist, J. Redström, and P. Ljungstrand, "TokenBased Access to Digital Information," Proceedings of HUC'99 (1999), pp. 234–245
6. Amex to Implement Digital Tokens to Replace Cards, http://www.infosecurity-magazine.com/news/amex-to-implement-digital-tokens/
7. Rajdeep Borgohain, Chandrakant Sakhatwade, Sugata Sanyal, "TSET: Token based Secure Electronic Transaction", IJCA, Volume 45 – Number 5, 2012.
8. Kanta Matsuura, Hideki Imai, "Digital timestamps for dispute settlement in electronic commerce: Generation, Verification and renewal", CiteSeerx, 2002
9. Shazia Yasin, Khalid Haseeb, Rashid Jalal Qureshi, "Cryptography based E-Commerce security: A Review", Volume 9, Issue 2, IJCSI, March 2012
10. L. Damgard. "Collission-free hash functions and public-key signature schemes." In Advances in Cryptology – Eurocrypt'87, pp. 203–217. Springer-Verlag, LNCS, vol. 304, 1988.
11. S. Josefsson, SJD, "The Base16, Base32, and Base64 Data Encodings", RFC 4648,Network Working Group, October 2006.
12. MongoDB-Documentation. http://docs.mongodb.org/manual/tutorial/
13. eSign – Online Electronic Signature Service, http://www.cca.gov.in/cca/?q=eSign.html, Last accessed May 12, 2017.